CSC-EPL-89/009

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

PYRAMID DEVELOPMENT CORPORATION

PC / DACS

28 September 1989

FINAL EVALUATION REPORT

PYRAMID DEVELOPMENT CORPORATION

PC/DACS

NATIONAL COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

September 28, 1989

CSC-EPL-89/009
Library No. S235,424

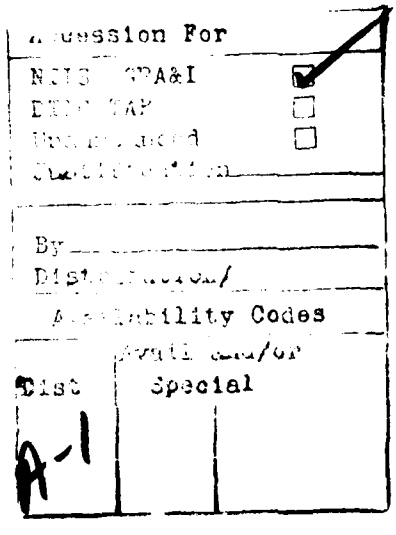
FOREWORD

This publication, the Final Evaluation Report of Pyramid's PC/DACS, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center". The purpose of this report is to document the results of the PC/DACS evaluation. The requirements stated in this report are taken from the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION of the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA* dated 16 September 1988.

Approved:

September 28, 1989

Thomas R. Malarkey,
Deputy Chief,
Office of Product Evaluations
and Technical Guidelines
National Computer Security Center



ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals, who were provided by the following organizations:

Kris C. Rogers

Kenneth D. Vane

MITRE Corp. (CSD)
7525 Colshire Drive
McLean, Virginia 22102-3481

Myron Coplin

National Computer Security Center

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

The team would like to thank Captain Deborah M. Clawson, USAF for her early work on this evaluation.

EXECUTIVE SUMMARY

The National Computer Security Center (NCSC) examined the security protection mechanisms provided by Pyramid's PC/DACS Rel 2. PC/DACS is a subsystem not a complete trusted computer system. Therefore, it was evaluated against the *Computer Security Subsystem Interpretation* (CSSI). Specifically, the applicable requirements for this evaluation included identification & authentication (I&A), discretionary access control (DAC), audit and object reuse.

PC/DACS runs on an IBM PC, XT or AT or 100% BIOS compatible microcomputer with at least 512KB of random access memory (RAM) running MS-DOS or PC-DOS 2.0 or greater. The system is required to have at one floppy disk drive, a hard disk drive and a monitor. PC/DACS is intended for environments where several users share a single personal computer.

The evaluation team determined that the highest class at which PC/DACS satisfies the I&A, DAC, audit and object reuse requirements of the CSSI is class D although PC/DACS meets some individual features at higher levels. The overall D rating in each function resulted from PC/DACS's inability to meet all the features, assurance and documentation requirements as specified in the CSSI.

Subsystems are designed to be installed on automatic data processing (ADP) systems. Specifically, subsystems are designed to add a level of protection to an ADP system that has limited or ineffective security mechanisms. However, subsystems are not intended to protect any information on an ADP system which processes classified or sensitive information. This is because subsystems may not be capable of maintaining the integrity of classified or sensitive information which is required of such systems. Therefore, subsystems may not be added to a trusted system for the sole purpose of processing classified or sensitive information.

INTRODUCTION

In May 1989, the National Computer Security Center (NCSC) began a product evaluation of Pyramid Development Corporation's PC/DACS. The objective of this evaluation was to rate PC/DACS against the *Computer Security Subsystem Interpretation* (CSSI), and to place it on the Evaluated Products List (EPL) with a final rating for each of PC/DACS's components. This report documents the results of the evaluation. This evaluation applies to PC/DACS Rel 2 available from Pyramid Development Corporation.

Material for this report was gathered by the NCSC PC/DACS evaluation team, through documentation, interaction with system developers, and through the use of PC/DACS.

Evaluation Process Background

The National Computer Security Center (NCSC) was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of Trust Technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program, the Center works with the manufacturers of hardware and software products to implement and make available to the public good computer security solutions. Under this program, the NCSC evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations.

Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may they be used as justification for processing classified material.

Subsystems considered in the program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria.* Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog.*

Document Organization

This report consists of four major sections and three appendices. Section 1 is an introduction. Section 2 provides an overview of the system's hardware and software architecture. Section 3 provides a mapping between the requirements specified in the CSSI, and the features and assurances that fulfill those requirements. Section 4 presents the evaluation team's comments of the subsystem. The appendices identify specific hardware and software components to which the evaluation applies, and also a glossary of terms.

SYSTEM OVERVIEW

Pyramid was founded in February 1985 to provide professional data processing services to Corporate clients for micro application development. Pyramid is a products and services company, developing and marketing corporate PC management software products for IBM and IBM compatible personal computers. Currently, Pyramid develops, manufactures, markets, and supports a micro- security product: PC/DACS for IBM and IBM compatible personal computers and a network security product Net/DACS, Novell version.

The system that was evaluated was PC/DACS Rel 2 that runs in single user environment. PC/DACS is runs on an IBM PC XT or AT or a 100% BIOS compatible microcomputer with at least 512KB of random access memory running MS-DOS or PC-DOS 2.0 or greater. The system is required to also have at least one floppy disk drive, a hard disk drive and a monitor. PC/DACS was developed in response to needs defined by one of Pyramid's corporate clients, a large insurance company, to protect corporate information residing on employees' personal computers. PC/DACS protects data when several users are sharing a single IBM personal computer. The insurance company served as a Beta test site and the PC/DACS stand alone product was installed on a corporate wide basis with plans to install the Local Area Network version upon completion. Pyramid expects to put out new releases every six months.

The team met with the vendor in June of 1989. The evaluation formally began with the receipt of the PC/DACS Rel 2 software in August 1989. The team reviewed vendor documentation, tested the PC/DACS software at the DOS and BIOS levels, and wrote a Preliminary Evaluation Report for review by Pyramid.

Security Relevant Portion

The protection-critical mechanism or the Security Relevant Portion (SRP) of PC/DACS, consists of its hardware and software capabilities. A description of these components and their security relevant roles are described in the following two sections.

Hardware Architecture

PC/DACS requires a IBM PC/XT, AT or 100% compatible computer. The team used three hardware platforms during the analysis and testing of the system. An IBM PC at MITRE in Washington, DC and an IBM XT and AT at the National Computer Security Center (NCSC) in Linthicum, MD. Because the vendor does not modify the hardware or add any hardware for its implementation of the TCSEC requirements, we will present the standard hardware architecture of the 8088 (used in the IBM PC) through the 80386 as it relates to the DOS environment.

The DOS environment was built around the Intel 8088 chip which is a single- state processor. All processors of the 80xxx line are backward-compatible with this single-state processor. Each processor has a number of registers which it requires to perform all operations. The registers in the 8088 and 8086 are the same and include general purpose registers, pointer registers, index registers, segment registers and a flag register (Table 1).

General purpose registers are both 8 bit and 16 bit registers. The nX reference is for 16 bits and the nH reference is for the high-order 8 bits. The nL reference is for the low-order 8 bits. In the 80386 the registers are the same except they are 32 bit registers rather than 16 bit. The low-order 16 bits are addressed exactly the same way as before, however the entire 32 bit address uses an E as a prefix. For example AX gets the low-order bits and EAX gets the entire 32 bit register in which AX references the lower 16 bits. SP references the stack pointer's low-order 16 bits whereas ESP references the entire 32 bit stack pointer.

DOS requires the following resources from the hardware base:

- Boot Record

- ROM BIOS

When the system is initialized ROM BIOS is invoked and looks on drive A first and then the active partition of the fixed disk for a boot record. If not found, ROM BIOS branches to ROM BASIC. If it is found, then the boot record is read into memory and ROM BIOS branches to this boot record. The boot record then checks the root directory for IBMBIO.COM and IBMDOS.COM in order to boot DOS. The boot record is responsible for the remaining events to construct DOS and constitutes the first modifiable code of the DOS operating system. It must conform to certain standards before ROM BIOS will relinquish its control, but these standards are quite spoofable.

DOS can be ported to many platforms because ROM BIOS provides a common well-defined interface which performs many hardware specific actions on behalf of DOS. This prevents DOS from having to provide these unique utilities for each machine it supports. The BIOS is accessed via software interrupts 10H through 1AH. Parameters are passed through the microprocessor's registers and the BIOS routines are expected to preserve all other registers values upon returning. The BIOS interrupt functions are:

Int 10H Video functions are passed via different values of register AH

Int 11H Equipment installed bit map is returned in register AX

Int 12H Memory size is returned in AX (1KB blocks)

Int 13H Diskette functions are passed via different values in register AH

Int 14H Asynchronous communications functions are passed via different values in register AH. Data is usually passed via registers AL and DX.

Int 15H System Services requests are passed via different values of AH.

Int 16H Keyboard functions are passed via different values of register AH

Int 17H Printer support functions are passed via different values in register AH

Int 18H Rom Basic system

Int 19H Bootstrap loader reads track 0 sector 1 of drive on register DL into memory and sets the Instruction Pointer (IP) to 7C00H the location of the boot program.

Int 1AH System-timer and real-time clock services are passed via different values of register AH

DOS adds its own interrupts which are briefly described in the Software Architecture section.

Since the hardware must be a single-state machine (even though the 80286 and 80386 are actually capable of four states), all programs interface with the hardware as peers. Users of these systems should understand that anything DOS can do any other program can do. The standard hardware cannot protect fro· ı tampering the domain of any process, including DOS. It is only by conformirg to prescribed conventions that multiple programs (i.e., TSRs) can exist unimpaired on the system.

This leads to problems because any method of software protection must rely on secrecy of the methods used rather than enforcement by isolation. The TCSEC requires enforcement by isolation. Therefore all software solutions on a single state machine are incapable of meeting TCSEC requirements.

That said, until multi-state solutions are created for PCs, there still is value having software-based systems evaluated. This system does provide features which do significantly improve the security aspects of the system. The user should understand, however that these systems are compromisable.

The integrity checking of the hardware varies between vendors; however, most reputable vendors provide hardware diagnostic checks for these machines. These checks are sufficient to assert the hardware base is stable.

Software Architecture

This section describes the security relevant components of the PC/DACS's software.

PC/DACS is a software package that runs on versions 2.1 to 3.2. of the MS-DOS operating system.

PC/DACS consists of the following set of features:

1. Boot Protection

2. Low Level Disk I/O Protection

3. Workstation Timeout

4. EMS (LIM) Support (Loads Resident Monitor to Expanded Memory)

5. User Administration (For multiple User IDs)

6. Security Database Extract

7. DES Encryption Utility

8. Statistical Logging (Operational and Session Logging)

9. Violations Logging

10. View Manager (Users with Access Rules)

11. Resource (Subdirectory-Level) Encryption

12. Resource Password Protection

Installation

PC/DACS is installed from a floppy disk. The installation program:

1. Copies PC/DACS files to the hard disk,

2. Integrates the PC/DACS software into the boot sequence

3. Creates the system administrator's ID

There are three modes of installation:

1. Minimum installation

2. Maximum installation

3. Custom installation

Minimum installation provides Logon with User ID and password, Boot Protection, and Workstation Timeout. Minimum installation is only recommended for a single user system. Maximum installation installs all of the security features and is recommended for multi-user systems. Custom installation allows the selection of security features. The system was evaluated with all security features installed except encryption.

Logon with User ID and password are always provided and support the TCSEC requirement for identification and authentication. User Administration and View Manager support the TCSEC requirement for discretionary access control. Violations Logging and Statistical Logging support the TCSEC requirement for Audit. Other features such as Workstation Timeout support recommended security practice Low Level Disk I/O

Protection and Encryption make it more difficult for a user to circumvent PC/DACS, and provide additional protection. However, because they are software-based and the team does not evaluate the strength of encryption algorithms, they are not sufficient to satisfy the TCSEC requirement for assurance.

Boot Protection

This feature is designed to prevent users from booting around PC/DACS and accessing any of the data on your hard disk at the DOS file system level. PC/DACS replaces the Master Boot Record with its own and controls the boot process. There are no modifications to DOS, the file allocation tables (FAT), or the disk directory structures.

The normal boot sequence for a PC is as follows:

1. The ROM BIOS code loads the Master Boot Record (MBR).

2. The MBR loads the DOS Boot Record (DBR).

3. The DBR loads the BIOS and DOS files.

4. DOS loads the Config.sys drivers followed by Command.Com.

5. The Command Interpreter reads the Autoexec.bat files and executes its contents.

PC/DACS controls the boot sequence by loading itself ahead of the MBR.

Because software boot protection cannot stop low level access by knowledgeable users, two types of transparent encryption features are provided for additional protection. (The team does not evaluate the strength of encryption algorithms.) Boot protection prevents access at the DOS file level. Full Disk Encryption (FDE) is available to provide read access protection at the BIOS level. FDE does not prevent the reading or writing to hard disk sectors through BIOS. The purpose of FDE is to prevent the reading of data in comprehensible form when PC/DACS is not resident because the PC has been booted from a floppy. FDE also encrypts the disk data structures such as the File Allocation Tables (FAT), directories, DOS Boot Records, all parts of DOS, and all of the data items on the disk. However, whole sectors or bytes in sectors can be randomly modified through the BIOS services or the hard disk contents can be destroyed through the use of a low level format program.

SRP Protected Resources

The SRP must provide protection by defining resources into two different classes. These classes are Subjects and Objects. Subjects are the active entities which make requests to the SRP. Objects are the passive entities which the SRP must protect from unauthorized access.

Subjects

Subjects defined by PC/DACS can perform all commands available to the processor. The subjects are of two classes:

- Users or
- Administrators

Both types of subjects exist on the system as the entire domain of the hardware. Administrators are the only privileged subjects and all administrators are equally as privileged. Privilege in this subsystem means that the SRP interfaces available to the subject allow the subject to violate the policy of the SRP. Users who are not administrators only have access rights which are granted by administrators. Individual users cannot grant access to other users even for objects which they create.

Objects

PC/DACS provides protection for the following objects:

- Communication Ports
- Printer Ports
- Floppy Disk Drives
- Directories and Subdirectories
- Files

SRP Protection Mechanisms

PC/DACS implements all four features available to subsystems: Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit.

Identification and Authentication (I&A)

At the end of the boot sequence, PC/DACS displays a logon screen. To logon, the administrator or user inputs a user identifier and password. The user identification is used in audit records providing for individual accountability.

The user may also input an optional project identifier. This used to determine the set of access privileges that the user will have for that session. A user may be associated with up to three projects.

There is a Global Security Parameter to set the number of access attempts that will be allowed. If the number of access attempts is exceeded, PC/DACS will either halt the PC or delay accepting any logon attempts for 60 seconds.

Additionally, PC/DACS provides a time-out feature which interrupts the subject's processing anytime the subject lets the computer idle for a administrator defined period. The time-out period can be set anywhere from one minute to nine hours fifty-nine minutes. A key sequence can also be defined to invoke immediate time-out. Time-out can be set to either lock the PC and wait for the current user to input their password, or logout the current user by rebooting the PC.

The system provides for a special class of user identification (userid) names. They are $GUEST and $DEFAULT. The $GUEST userid can be used to allow users access to unprotected objects. If /AUTOLOGON is added to the command line that invokes the DACS Resident Monitor in the AUTOEXEC.BAT file, PC/DACS will automatically log on to the guest ID and allow users to access the unprotected resources without having to logon through PC/DACS. There is no accountability if a user logs on as $GUEST, and the Trusted Facility Manual should specify that this option cannot be used for D2 operation. The $DEFAULT userid allows the system administrator to define a set of objects which all users will have access to by default.

Passwords are stored in an encrypted file in the PCDACS directory. The encrypted password file is not accessible to the normal user, but it is accessible to the system administrator.

Discretionary Access Control (DAC)

PC/DACS provides the capability for the system administrator to define access rules for system resources. One access rule can specify the permission rules for large groups of objects. With one access rule an administrator can protect a whole hard disk, a directory, a group of files, or one file for a particular user.

In addition to being able to define access rules for individual users, access rules may also be defined:

By project

- By default using User ID $DEFAULT

- For guest users using User ID $GUEST

Access rules may be defined by project rather than individual. If a User logs on to a project, the project's access rules are loaded. The default access rules are loaded first and apply if they are not replaced by personal or project access rules.

Access Control by Class of Object

Each class of object has different rules for access. They are:

- Ports: Each port can be made accessible or not accessible.
- Floppy Drives: All floppies can be inaccessible, read only, write only or read and writable.
- Files and Directories: Each file or group of files can have a set of access privileges defined for a particular User ID or Project ID. These access rights are discussed below.

File and Directory Access Rights

The following file access rights are provided:

- READ - read a file
- WRITE - write to a file
- OPEN - open a file
- CREATE - create a file
- DELETE - delete a file
- PURGE - Overwrite, then delete a file
- ADMINISTRATE - Make or remove sub-directories
- SEARCH - Search a sub-directory
- MODIFY - Rename a file
- EXECUTE - Execute a .COM or .EXE file

Most possible combinations of privileges can be defined, but there are some mutual dependencies. A user cannot be given the READ or WRITE privilege without the OPEN privilege. A user cannot be given the CREATE privilege without the WRITE privilege. A user can only be given the PURGE or DELETE privilege, but not both. Some degree of object reuse protection is provided if users are given the PURGE privilege rather than the DELETE privilege.

Rules for Defining Access on Groups of Files

The rules and syntax for defining access on groups of files are well- documented. The following rules are used to determine which access rule has higher priority:

Rule 1: File extensions are more significant than filenames for access rules.

Rule 2: In any file name or file extension, matching file string and access rule length is more significant than longer access rules. This gives the administrator the ability to define access to file groups based on the length of their file names or extensions.

Rule 3: In any file name or file extension that contains DOS global filename characters or wildcard characters, the left most characters are more significant than the characters farther to the right. This allows the administrators to easily define access to file groups by starting character string.

Loading Access Rules

PC/DACS builds a user's view by loading their access rules from the Security Database when they logon. The view they get is entirely defined by their assigned access rules, except every user is given minimal access to what is required to log on and off from PC/DACS and to use DOS internal commands.

The sequence in which the access rules are loaded is as follows:

1. The view for $DEFAULT is loaded if that user exists.

2. The user's project view or personal view is loaded. The user's personal view is loaded if the project field was left blank on the Logon screen. The project view is loaded if the user logged into a project.

This load sequence can be used to cancel access rules that are in the default view for particular users.

Object Reuse

PC/DACS provides some object reuse protection by allowing the administrator to give only PURGE access rights and never to grant DELETE access rights. If the user is given PURGE access rights, the file is overwritten before it is deleted. Whereas, DELETE access allows the user not to overwrite the file before it is deleted.

A user may be given either PURGE or DELETE access rights, but not both. If the user is given PURGE access rights, the file is overwritten before it is deleted. The Trusted Facility Manual should state that users should always be given PURGE access rights rather than DELETE access rights so that the memory space occupied by the file will not contain any data from the file when it is allocated to another user or program.

PC/DACS clears unallocated memory areas between users.

PC/DACS Rel 2 does not overwrite memory between EOF and EOC.

Audit

PC/DACS Rel 2 has the capability to record events in the audit trail and generate a report. The events that can be audited fall into two categories: Statistics and Violations:

Statistics include the following events:

- User Logon
- User Logoff
- User Re-logons after Timeout
- User Timeout
- Program Start (Load and Execute)
- Program Exit
- Program Exit and Stay Resident
- Create a Subdirectory
- Remove a Subdirectory
- Open a File
- Create a File
- Write to File
- Delete a File
- Rename a File
- Change a File Mode
- Change Password
- Add Local Password

- Printer Access
- COM: Port Access

Violations include the following events:

- Logon User ID NOT Found
- Logon Password Error
- Resource Password Error
- Attempt to Write to Printer
- Attempt to Access COM: Port
- Unauthorized Read Attempt
- Unauthorized Write Attempt
- Unauthorized Open Attempt
- Unauthorized Create Attempt
- Unauthorized Delete Attempt
- Unauthorized Rename Attempt
- Unauthorized Make Directory Attempt
- Unauthorized Remove Directory Attempt
- Unauthorized Program Exec Attempt
- Unauthorized Modify File Attempt
- Unauthorized Disk Format Attempt

The TCSEC requires that all security relevant events be audited including:

- Use of identification and authentication mechanisms
- Introduction of objects into a user's address space
- Deletion of objects
- Actions taken by computer operators and system administrators

The statistic log records authorized events such as logon and file/directory creation or deletion. The violations log records unsuccessful events. The administrator's actions are not audited.
Each audit trail entry contains the following:

- User ID
- Project ID (if any)
- Event ID
- Date
- Time
- Sub directory name for directory create or removal
- File name for violations

The report generator can either display or print audit log reports. The selection criteria are as follows:

- Event Type - All, Statistics, or Violations
- Event ID - To select specific events
- Project ID
- User ID

Users must be prevented from modifying the system clock, because the audit data uses the system clock to timestamp audit records. If the system clock can be changed at will the benefit of the audit data is severely compromised. Pyramid states that there is an installation option that protects the system clock at the DOS and BIOS level, although it is bypassable by a very knowledgeable user. Changes to the clock by anyone should be audited.

EVALUATION AS AN I&A, DAC, AUDIT, AND OBJECT REUSE SUBSYSTEM

This chapter of the report analyzes PC/DACS's I&A, DAC, audit, and object reuse feature requirements and the CSSI assurance and documentation requirements. The comparisons are made against the requirements at the highest level at which the evaluation team has determined PC/DACS to satisfy. Where PC/DACS does not satisfy a requirement, the minimum requirement is stated and the deficiency explained.

Finally each individual rating is accumulated and a final feature rating is given for the four features I&A, DAC, audit, and object reuse. For this summary turn to Final Conclusion.

Identification and Authentication

Requirement

> The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Interpretation

- D1

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

- D2

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

Applicable Features

PC/DACS satisfies the following I&A/D2 features requirements:

- Users must identify themselves before they can access protected objects.

- Passwords are used to authenticate the user's identity.

- Passwords are protected by the subsystem.

- Individual accountability is enforced.

Conclusion

PC/DACS satisfies the D2 Identification and Authentication requirement.

Discretionary Access Control

Requirement

> The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Interpretation

D1:

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

2.1.3.1.1 Identified users and objects

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/D1, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to: access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

2.1.3.1.2 User-specified object sharing

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).

2.1.3.1.3 Mediation

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows access.

D2:

The following interpretations, in addition to the interpretations for the DAC/D1 Class, shall be satisfied at the DAC/D2 Class.

2.1.3.2.1 Single-user access granularity

The DAC/D2 class requires individual access control; therefore, the granularity of user identification must enable the capability to discern an individual user. That is, access control based upon group identity alone is insufficient. To comply with the requirement, the DAC subsystem must either provide unique user identities through its own I&A mechanism or interface with an I&A mechanism that provides unique user identities. The DAC subsystem must be able to interface to an auditing mechanism that records data about access mediation events. The evaluation shall show that audit data is created and is available to the auditing mechanism.

2.1.3.2.2 Authorized user-specified object sharing

The ability to propagate access right to objects must be limited to authorized users. This additional feature is incorporated to limit access rights propagation. This distribution of privileges encompasses granting, reviewing, and revoking of access. The ability to grant the right to grant propagation of access will itself be limited to authorized users.

2.1.3.2.3 Default protection

The DAC mechanism must deny all users access to object when no explicit action has been taken by the authorized user to allow access.

Applicable Features

PC/DACS provides DAC/D2 functionality. The following DAC/D2 features requirements are met: (1) Single-user access granularity, (2) Authorized user- specified object sharing, and (3) Default protection. Access control can be specified and audited based upon user identification. Only administrators are allowed to grant access rights. If no access rights are specified to a file or directory, the default is no access.

Conclusion

PC/DACS satisfies the Discretionary Access Control D2 feature requirement. PC/DACS does not satisfy the DAC/D3 feature requirement because it does not support the capability to specify a list of users or group for which no access is to be given.

Audit

Requirement

> The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Interpretation

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied re auditing subsystems at AUD/D2.

2.4.3.1.1 Creation and management of audit trail

The auditing subsystem shall create and manage the audit trail of security-relevant events in the system. If the other portions of the system are unable to capture date about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store date about events if the other portions of the system are capable of creating such data and passing them on.

2.4.3.1.2 Protection of audit data

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

2.4.3.1.3 Access control to audit

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

2.4.3.1.4 Specific types of events

Data about all security relevant events must be recorded. The other portion of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

2.4.3.1.5 Specific information per event

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

2.4.3.1.6 Ability to selectively audit individuals

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

Applicable Features

It is the team's opinion that the following security-relevant events must also be audited:

- Modification of the system clock.

- The use of each DACS event.

Each DACS event must be auditable because it reflects the actions of a privileged user, an explicit requirement of the TCSEC and CSSI. Inherit to this requirement is the need to keep an accurate timestamp. PC/DACS does not properly protect the system clock which is used to create the audit timestamp. If the system clock can be changed the benefit of the audit data is severely compromised.

Conclusion

PC/DACS does not satisfy the D1 feature requirement for audit.

Object Reuse

Requirement

> All authorizations to the information contained within a storage object shall be revoked *prior to initial assignment, allocation, or reallocation* to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Interpretation

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

Applicable Features

The purpose of object reuse is to prevent a subject from accessing the contents of an object after the object is relinquished back to operating system. This includes deleted files and directories and all memory after logging off.

For object reuse of files, PC/DACS provides some object reuse protection by allowing the administrator to give only PURGE access rights and never to grant DELETE access rights. In DOS, the deletion of a file means to place a space in the first byte of the filename field of the Catalog. DOS considers catalog entries (files) which start with a space as freed. However the file's data remains undisturbed. If the user is given PURGE access rights, the file is overwritten before it is deleted. Whereas, DELETE access allows

the user to follow the normal DOS delete routine and not to overwrite the file before it is deleted.

The system clears unallocated user memory areas between users, however allocated memory (i.e., Terminate and Stay Resident (TSR) programs) are not freed. The vendor says they will address this problem in their next release.

Object Reuse must be an automatic event of the system, it is acceptable that the system may have to set a configuration parameter on to enable Object Reuse. However requiring that the administrator to set PURGE rather than DELETE is not acceptable, because it requires an inordinate amount of effort and it is not verifiable or auditable.

Conclusion

PC/DACS does not satisfy the object reuse requirement for D2 and will receive a D rating for object reuse.

System Architecture

Requirement

> The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

- D1

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

Applicable Features

There are two components to this requirement. The first is domain protection and the second is the objects of the subsystem can be a defined subset.

Domain Protection

The following components make up the TCB subsystem:

- Password file

- DACS software

- System Clock

- Audit log

The evaluated system does not protect these components from external tampering. Therefore, PC/DACS does not satisfy the domain protection requirement for D1.

Defined Subset

The defined subset requirement allows the vendor to select only a subset of the set of all objects the system recognizes. This requirement removes the obligation for the evaluation team to determine what the real set of objects are and allows us to focus our attention only on the objects which the vendor chooses to include.

This software product runs under DOS on the entire line of IBM 100 percent compatible machines. This is a single-state machine (8088/8086) operating system. It makes absolutely no claims to provide domain protection in the memory used by the processor. The Subsystem Interpretation for D1 states:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform.

PC/DACS does not meet the D1 requirements for System Architecture because it is not designed to provide Domain Protection and the host operating system (DOS) does not support this concept.

Conclusion

PC/DACS does not satisfy the D1 System Architecture requirement.

System Integrity

Requirement

> Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Interpretation

- D1

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirements applies to all subsystems evaluated at any class, regardless of the functions they perform.

Applicable Features

This requirement is the same between D1 and D2. Pyramid claims there is no software to assess correct operation of the on-site hardware and firmware. The team feels that this requirement could be accomplished by the standard Boot Diagnosis available by the system reference disk. We feel that this is enough for this requirement.

Conclusion

PC/DACS satisfies the D2 Integrity requirement on all hardware platforms which provide Boot Diagnosis for hardware self-assessment.

Security Testing

Requirement

> The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB.

Interpretation

- D1

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

Applicable Features

The evaluation team tested PC/DACS using two major areas of concentration. The first area of testing was functional testing. This testing concentrated on providing the team assurance that PC/DACS's protection mechanisms function properly. The second phase of testing is aimed at determining if there are no apparent ways to bypass the security mechanisms of PC/DACS.

Phase one testing was functional testing performed at the DOS level. The testing consisted of developing a number of tests scripts that would exercise PC/DACS's DAC, I&A, and Audit mechanisms. These tests consisted of setting up PC/DACS with a number of users; attempting to access files that the users have the right to access and do not have rights to access; and studying the audit files for correct format. PC/DACS basically performed as expected, however, the administrative (ADMIN) privilege did not work correctly. In test cases where users were created with all access rights including ADMIN to a particular directory, the user was unable to create a sub-directory under directories that they have valid access rights to. According to the documentation users with the administrative (ADMIN) privilege should be able to create sub-directories.

Phase two testing consisted of looking for obvious flaws that would bypass the system's protection mechanisms using low level BIOS programs or DOS. The evaluation team was able to access system resources at the DOS level that corrupted the audit log of PC/DACS. The evaluation team also attempted to access system objects using low level utility programs, such as Norton Utilities. For the most part PC/DACS was able to prevent unauthorized access of these objects and the use of the utility program. However, the evaluation team was able develop a low level program, that accessed all of the files on the system by performing a complete read of the hard drive despite PC/DACS's protection mechanisms.

Conclusion

PC/DACS does not satisfy the D1 Security Testing requirement.

Security Features User's Guide

Requirement

> A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Interpretation

- D1

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

- D2

There are no additional requirements at the D2 Class.

Applicable Features

The user's guide and the simplicity of the actual interface make this subsystem user-friendly and effective in helping the user understand his domain. The Trusted Facilities Manual (TFM) contains most of the information on the protection mechanism because this subsystem requires an administrator to define each user's access rights. The unprivileged user cannot grant access; therefore, it is inappropriate for this to be discussed in the SFUG.

Conclusion

PC/DACS satisfies the D2 Security Features User's Guide requirement.

Trusted Facility Manual

Requirement

> A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

Interpretation

- D1

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

Applicable Features

The manual is extremely frank about the vulnerabilities of the system and what a system administrator can do to protect the system. The system provides a number of ways to examine the audit files. The requirement for the detailed audit record structure is not

provided; however, the team feels that the audit query language and the data provided meets the intent of this requirement.

The team feels that the system must not be configured with the $GUEST option in place. The TCSEC and CSSI require each user have a unique ID for auditing. This will have to be added to the manual.

Conclusion

Assuming the manual is modified to say that $GUEST user must not be installed on the evaluated system then PC/DACS satisfies the D2 Trusted Facility Manual requirement.

Test Documentation

Requirement

> The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Interpretation

- D1

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

Applicable Features

Pyramid does not have a formal test document. This is not unusual for PC subsystem vendors. In the future they plan to develop a test plan and document.

Conclusion

PC/DACS does not satisfy the D1 Test Documentation requirement.

Design Documentation

Requirement

> Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this

philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

- D1

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

Applicable Features

Conclusion

Although not in one comprehensive document, the PC/DACS design is well documented and has a clear (although flawed) philosophy of protection which the subsystem enforces. Therefore, PC/DACS satisfies the D2 requirements for Design Documentation.

Rating Assignment

This section describes the composite feature rating and how it is determined. The composite rating for each evaluated feature is based upon the individual ratings awarded as previously described. These individual ratings are combined with ratings for assurances, documentation, and "supporting functions" (see discussion below). The resulting composite rating is equal to the lowest rating awarded in any one of the individual ratings or "supporting functions".

The CSSI requires that subsystems have "supporting functions" because the requirements rely on one another (e.g. an auditing subsystem needs the identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

a. The supporting function is provided by another feature of the subsystem
b. The supporting function is provided within the feature, even though it may duplicate an aspect of another feature
c. The supporting function is provided through an interface to other products

The "supporting function" must be at the same level as that of the feature to obtain the resulting rating.

Taking the values attained in Section 3 (above), the composite ratings for each of the features of PC/DACS are derived as shown in table 1. Note that PC/DACS provides the

supporting functions by integrating them within the feature. Since PC/DACS does not provide all of the required assurance, documentation and supporting functions, PC/DACS will be placed on the EPL as a D1 I&A, D1 DAC, D Auditing, and D Object Reuse Subsystem.

TABLE 1

EVALUATED FEATURE	INITIAL FEATURE RATING	LOWEST RATING (ASSURANCE)	LOWEST RATING (DOCUMENTATION)	REQUIRED SUPPORTING FUNCTION	SUPPORTING FUNCTION RATING	COMPOSITE FEATURE RATING
I&A	D2	D	D	AUDIT DAC*	D Yes	D
DAC	D2	D	D	I&A	D2	D
AUDIT	D	D	D	I&A DAC*	D2 Yes	D
OR	D	D	D			D

* Audit and/or authentication data must be protected through DAC or domain isolation. Isolation is defined as any mechanism which prevents a subject from accessing the processes or data structures which provides the feature.

EVALUATOR'S COMMENTS

This section allows the evaluators to comment on features which the TCSEC does not require, but which the user of these systems may find useful or needed for the administration or use of the subsystem.

The team feels that the PC/DACS Rel 2 does provide a level of security which the PC running DOS lacks. The database extract feature allows a vendor to load audit and access data into a file which can then be process by the user's favorite database package. We liked this feature because it allowed the team to be able to produce hardcopy audit trails of test cases. The user will no doubt find this feature equally as useful.

The menu system and documentation was friendly; however, it could be friendlier. Specifically, the number of panels which an administrator must pass through to change the access control lists of a user is 4 if you remember the userid and many more if you do not remember. If the system has only a few users this is not too bad but we defined around 30 different users. Access modification was by userid only. This means an administrator who is trying to prevent write access to a file for all users must page through each userid and copy these down on a piece of paper then go to the resource assignment screen to inquiry about each user's access rights. The team has found that an administrator will more likely be interested in viewing access rights by object rather than by subject. However, this software does not support this feature.

EVALUATED HARDWARE COMPONENTS

This appendix lists the Pyramid marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluation. The primary requirement from the vendor for hardware is that the hardware function properly while running DOS 2.0. This was verified by the diagnostic tests (see page 3, "Hardware Architecture") performed to verify the hardware for DOS 100 percent compatibility.

To operate in correspondence with the I&A, DAC, and Audit ratings, the security subsystem must contain the hardware components listed in this section.

The system covered by this evaluation is the IBM PC, XT and AT running DOS 2.1 through 3.2 with a system clock and a hard drive.

EVALUATED SOFTWARE COMPONENTS

PC/DACS is designed to run on versions 2.1 to 3.2. of the MS-DOS operating system.

The PC/DACS Rel 2 software was evaluated. The software was delivered on five 5 1/4" floppy disks consisting of an install disk and disks 1-4. The software consisted of the files listed below plus 51 .HLP files and 15 .OVL files all dated 8-01-89:

Install Disk:	Disk 1:	Disk 2:	Disk 3:	Disk 4:
DACSRES.EXE	UNLOCK.BAT	PCSADMNS.EXE	PCSENC.EXE	PCSDECTL.EXE
INSTALL.EXE	PCSBTPRT.EXE	PCSUMS.EXE	CK.EXE	PCSDEXTG.EXE
PCSLGOFF.EXE	PCS.EXE	PCSURS.EXE	PCSUVIEW.EXE	PCSDEXTL.EXE
DACS.PIF	PCSTMO.EXE	PCSPRS.EXE	PCSRPAUD.EXE	PCSDEXTP.EXE
INSTALL.PIF	PCDTMO.PIF		PCSRPCTL.EXE	PCSDEXTU.EXE
LOGOFF.PIF	PCSADGLB.EXE		PCSLOGRS.EXE	
PCS.PIF	PCSREMOV.EXE		PCSDES.EXE	
PCSLGOFF.PIF			PCS-DSK.DRV	
DACS.PRO				
DRVTBL.PRO				
WINSTALL.PRO				
PCSRMDEV.SYS				
DACS-CGA.VID				
DACS-EGA.VID				
DACS-STD.VID				
DACS-TXT.VID				
DACS-VGA.VID				

GLOSSARY

ADP	Automatic Data Processing
AH	Accumulator High-order 8 bits
AL	Accumulator Low-order 8 bits
AX	Accumulator Full 16 Bits
BIOS	Basic Input/Output Services
CSD	Civil Systems Division (A Division of MITRE)
CSSI	Computer Security Subsystem Interpretation
DAC	Discretionary Access Control
DBR	Dos Boot Record
DES	Data Encryption Service
DH	Data Register High-order 8 Bits
DL	Data Register Low-order 8 Bits
DoD	Department of Defense
DOS	Disk Operating System
DX	Data Register 16 Bits
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMS	Extended Memory Service
EPL	Evaluated Products List
ESP	Extended Stack Point Register 32 Bits
FAT	File Access Table
FDE	File Data Encryption
I&A	Identification and Authentication
IBM	International Business Machines
IP	Instruction Pointer
MAC	Mandatory Access Control
MBR	Master Boot Record
MS-DOS	MicroSoft Disk Operating System
NCSC	National Computer Security Center
NET/DACS	Network version of PC/DACS
Novell	A network standard
NSDD	National Security Decision Directive
PC	Personal Computer
PC/DACS	Personal Computer/Discretionary Access Control System
RAM	Random Access Memory
ROM	Read Only Memory
SFUG	Security Features Users Guide
SP	Stack Pointer
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TSR	Terminate and stay resident
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual
USAF	United States Air Force

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT **UNLIMITED DISTRIBUTION**
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) **CSC-EPL--SUM-89/009**	5 MONITORING ORGANIZATION REPORT NUMBER(S) ~~S232,424~~ S 235424
6a NAME OF PERFORMING ORGANIZATION **National Computer Security Center** / 6b OFFICE SYMBOL (If applicable) **C12**	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State and ZIP Code) **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	7b ADDRESS (City, State and ZIP Code)
8a NAME OF FUNDING SPONSORING ORGANIZATION / 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State and ZIP Code)	10 SOURCE OF FUNDING NOS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO
11 TITLE (Include Security Classification) **Final Evaluation Report PYRAMID PC/DACS**	
12 PERSONAL AUTHOR(S) **Kris C. Rogers Kenneth D. Vane, Myron Coplin**	
13a TYPE OF REPORT **Final** / 13b TIME COVERED FROM ____ TO ___ / 14 DATE OF REPORT (Yr, Mo, Day) **890928** / 15 PAGE COUNT **43**	
16 SUPPLEMENTARY NOTATION	

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB GR	**NCSC, I&A, DAC, AUDIT PYRAMID, PC/DACS, CSSI**

19 ABSTRACT (Continue on reverse side if necessary and identify by block number)

The National Computer Security Center (NCSC) examined the security protection mechanisms provided by Pyramid's PC/DACS Rel 2. PC/DACS is a subsystem, not a complete trusted computer system. Therefore, it was evaluated against the *Computer Security Subsystem Interpretation* (CSSI). Specifically, the applicable requirements for this evaluation included Identification & Authentication (I&A), discretionary access control (DAC), audit, and object reuse. The evaluation team determined that the highest class at which PC/DACS satisfies the I&I, DAC, audit and object reuse requirements of the CSSI is class D although PC/DACS meets some individual features at higher levels. The overall D rating in each function resulted from PC/DACS's inability to meet all the features, assurance and documentation requirements as specified in the CSSI.

This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21 ABSTRACT SECURITY CLASSIFICATION **UNCLASSIFIED**	
22a NAME OF RESPONSIBLE INDIVIDUAL **DENNIS E. SIRBAUGH**	22b TELEPHONE NUMBER (Include Area Code) **(301)859-4458**	22c OFFICE SYMBOL **C12**